Notice of Allowability	Application No.	Applicant(s)	
	10/066,041	COPPERSMITH ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *01/08/2007*.

2. ☒ The allowed claim(s) is/are *1-20*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

Allowable Subject Matter

1. Claims 1-20 are allowed.

2. The following is an examiner's statement of reasons for allowance:

The primary reasons for the allowance of the independent claims 1, 9, 17, 19 and 20 are the inclusion of the following limitations that are not found in the prior art and they are uniquely distinct features. The closest prior art is Coppersmith et al. (5,454,039). Coppersmith discloses a method to provide a software-efficient pseudorandom function for mapping an index and a key to a pseudorandom sequence of bits.

However, this art fails to anticipate or render the following limitations:

"Claim 1: one or more mask tables produced from one or more of the initial keys, each of the mask tables having one or more masks, one or more of the masks being combined, in each respective step, with the respective new evolving state in a combination operation to create a respective step output, the random output stream being a concatenation of all the respective step outputs, and one or more of the masks in the mask tables being replaced by one or more replacement masks after the combination operation is performed a predetermined number of times, the replacement masks not being linear combinations of prior masks".

"Claim 9: two or more mask tables produced from one or more of the initial keys, each of the mask tables having one or more masks, one or more of the masks from

each table being combined, in each respective step, with the respective new evolving state in a combination of all the respective step outputs".

"Claims 17 and 19: B. producing one or more mask tables from one or more of the initial keys, each of the mask tables having one or more masks;

C. applying a round function to a current evolving state to produce a respective new evolving state;

D. replacing the current evolving state with the new evolving state;

E. combining one or more of the masks with the current evolving state in a combination operation to create a respective step output;

F. replacing one or more of the masks in the mask tables by one or more replacement masks after a number of combination operations, the replacement masks not being linear combinations of prior masks;

G. repeating steps C through F one or more times;

H. concatenating all the respective step outputs to create the random output stream".

"Claim 20: B. means for producing one or more mask tables from one or more of the initial keys, each of the mask tables having one or more masks;

C. means for applying a round function to a current evolving state to produce a respective new evolving state;

D. means for replacing the current evolving state with the new evolving state;

E. means for combining one or more of the masks with the current evolving state in a combination operation to create a respective step output;

F. means for replacing one or more of the masks in the mask tables by one or more replacement masks after a number of combination operations, the replacement masks not being linear combinations of prior masks;

G. means for repeating steps C through F one or more times;

H. means for concatenating all the respective step outputs to create the random output stream".

3. The dependent claims 2-8, 10-16 and 18 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A.N.

February 14, 2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100